Exhibit A

Provisional Patent Disclosure:

"System and Method for efficient information distribution and data collection in location aware communication networks"

Inventors:

Scott Sturges Andrews, Petaluma, CA, and
Axel Fuchs, San Jose, CA

Both of Inventero, LLC

Field of Invention:

The present invention is associated with network communications, specifically with the means by which messages conveyed by a network are routed to their intended recipient(s).

Background of the Invention:

The past two decades have seen a variety of attempts to apply location and communications technologies to automobiles and to various mobile applications. We have seen the development and worldwide deployment of computerized navigation systems that use various forms of digital map databases combined with graphical displays and high-powered data processors to present the user's current position on a graphical map. Handheld versions of these devices have also been developed, some of which include wireless data communications to provide traffic and other location related information on the map display. These developments, generally known as Intelligent Transportation Systems (ITS) also include various types of collision warning and vehicle information systems that provide improved information to drivers of motor vehicles, allowing them to better understand the roadway environment and therefore travel more safely and with less delay.

In parallel with these developments the Internet has grown and new Internet related applications have been developed to provide productivity, entertainment and other forms of services to users. Recently, the bandwidth and availability of wireless communications systems has merged with higher power processing, improved memory capability and improved display screen technology to support smartphones and other portable devices, which are able to access the Internet wirelessly and provide a wide variety of Internet related services to users as they move from place to place. These systems are characterized, generally, by a wide array of choices in the type and function of applications that may be installed and used.

With the decreasing cost of computing and communications, more and more mobile computing terminals are now attached to wireless networks. In particular, these systems are used to receive information provided by service providers, and also to collect data from the mobile environment which is then processed into information that may subsequently provided back to the mobile terminals by service providers.

Mobile data systems, specifically smartphones, wireless Personal Digital Assistants (PDAs), wireless tablet computers, wireless enabled navigation devices and systems, and related mobile devices typically provide mobile access to services, often via the Internet. While this is very useful, it carries some significant limitations. Specifically, to provide so called Location Based Services (services related to the specific location of the device), the system must either constantly track the location of the mobile device, or the device itself must constantly request location based services and include its location in each request. In situations where these requests are unique to the terminal, this is not a significant problem (for example requesting driving directions from a specific location) because generally not all terminals are requesting terminal specific information all the

time, and requests from any specific mobile terminal are likely to be infrequent. However this request-response characteristic of the Internet and the worldwide web, based on conventional addressed communications networks, results in severe inefficiencies for location based services involving large numbers of terminals within a specific area or locale. For example, if a service provider seeks to provide a message to only those terminals entering a retail establishment (or, perhaps only those passing by), it must somehow learn the addresses of each terminal in the desired location. One way to accomplish this is to program each terminal with appropriate actions for each and every location. However, since these actions will change over time, the terminals must constantly be updated. In addition, since the number of possible locations related to location based services is effectively unbounded (infinite number of locations, and an unbounded number of possible service providers), storing, updating and serving requests for this database would require huge amounts of data storage capacity, and huge amounts of communications bandwidth to both update ad to serve responses to requests. Another way to accomplish this is to have every mobile terminal regularly provide its location to a service provider as it moves about in order to allow the service provider to determine if there are any services available for or targeted to that location. Not only does this result in a massive level of requests for services (and, the finer the location specificity, the larger the number of requests), but, depending on the user's needs and preferences, and the availability of location based services, most of these requests are likely to result in a "no services for that location" result. In addition, since the location based request is sent to only a single service provider, accessing multiple services will result in multiple requests from the same location. In addition, there is no way for such a system to support a user who might be interested in spontaneous location based services, that is, unsolicited services that the mobile terminal is not pre-programmed to request. Providing mobile terminal location information on an ongoing basis also presents privacy issues, since this would allow the service provider to monitor the movements of the mobile terminal at all times and in all places.

It is possible to overcome the above issues by making the network geographically small. In this way, each location is specific to a particular network, so by joining a particular network, the terminal is able to then access services unique to the location of that network. While this approach mitigates the need for a large number of location-based requests, and also supports a potentially unbounded number of unique service providers, it suffers from other problems. Specifically, with a geographically small addressed network, mobile terminals (nodes) will enter and leave the local network (e.g. the hot spot) frequently. This means that a great deal of network overhead must be devoted to maintaining the local network by constantly updating all nodes about changes in the network addresses. Second, if a node (mobile terminal or service provider) wishes to send a message to all nodes in the local network, it must send the same message multiple times, once, to each node. While IP mechanisms exist for multicasting (sending a single message to all members of the network) this type of communications is difficult to control (for example dealing with overlapping radio coverage from adjacent networks), so it is seldom implemented in commercial systems. Where it might be implemented, the system still suffers from requiring the constant maintenance of the network in order to maintain a well-defined sub-net. If the network is enlarged so that the nodes do not enter

and leave as frequently, then it becomes less and less location specific, and the problems described above return.

These limitations arise from the fact that the conventional web based services are based on the Internet Protocol. This protocol defines, among other things a process for addressing devices connected to the a network so that one device can send data packets to any other device as long as both devices have appropriate network addresses. While this approach is highly useful, and it is responsible in large part for the explosive growth in the use of the Internet, it is inadequate in situations where the terminal addresses may not be known, when the location of terminal changes frequently, or when the network nodes in a localized network may change frequently; these situations represent a substantial portion of the potential operational envelope for mobile devices.

Various examples of these different geographic network scales exist. These are dominated by cellular networks (e.g. CDMA, GSM, GPRS, EDGE, CDMA 1xRT, CDMA 2000, EVDO, UMTS, LTE, etc.) and by stationary wireless networks (e.g. WiFi - IEEE 802.11a/b/g/p/n, WiMax - 802.16, and low bandwidth sensor networks IEEE 802.15).

Figure 1 shows a cellular core network infrastructure to connect mobile users to content providers over the network.

Cellular networks provide data connectivity to mobile users over a large area with seamless hand-off between cell towers. The average cell site serves a range of 10km around the cell tower. Thus thousands of mobile terminals may be in a certain cell at any time and the size of the cell is much larger than geographical area of relevance of most location based messages. While this architecture is useful for mobile access to the Internet, it suffers directly from many of the problems described above.

In GSM or WCDMA networks, the GPRS tunneling protocol (GTP) is the defining IP protocol of the GPRS core network. Primarily it is the protocol which allows end users of a GSM or WCDMA network to move from place to place while continuing to connect to the Internet as if from one location at the Gateway GPRS Support Node (GGSN). It does this by carrying the subscriber's data from the subscriber's current Serving GPRS Support Node (SGSN) to the GGSN which is handling the subscriber's session and send/receive data to the mobile terminal over the radio network.

However, this communication which occurs within one network is less standardized and may, depending on the vendor and configuration options, use proprietary encoding or even an entirely proprietary system. In addition, no information about the actual location of the cell tower or the mobile terminal is available to content providers and content aggregators.

Stationary (i.e. non cellular) networks provide high bandwidth low cost connectivity, but because they are also address based, they also suffer from the problems described above. WiFi transmitters typically provide a radio range of less than 100 m (often much less than

100 m), so these networks provide good location specificity, but this small geographic size means that mobile users are constantly moving in and out of the network. For an automobile based mobile terminal traveling at 60 mph, and WiFi network with a range of, for example 30 meters, a mobile terminal will only be inside the network range for 2 seconds. The WiFi network setup time typically requires about 10 to 15 seconds, so the network will never be stable enough to support any meaningful level of data communications.

WiMAX provides a substantial increase in range, so the network management problem is not a concern, but the large area results in many users (many more than WiMAX is typically able to support, and the same issues with large numbers of location based requests described for cellular applies to WiMAX.

While the Internet Protocol includes provision for multi-casting, that is sending a packet to all nodes on the network, this feature is not widely implemented for the simple reason that the Internet is so large that worldwide multicasting would cause havoc ranging from uncontrollable spam (unwanted messages) to huge bandwidth demands from messages traveling through every node on the network. Because of this, the multicasting feature of the Internet protocol is typically limited to a small subset of nodes in a local region of the network. So, in effect a node might be able to multicast to the other nodes locally connected to the same network (what is often referred to as a sub-network), it is not generally able to multicast beyond this limit. A sub-network might, for example, be formed by a group of wireless devices all connected to the same wireless hub, or even a group of cellular phones connected to the same cellular base station. In the cell phone case, multicast is generally also not allowed even within this sub-net simply because the systems doesn't generally need this feature, and the number of cell phones in the radio footprint of a single cellular base station may be very large. Also, in situations where mobile terminals may enter or leave a sub-net regularly, the need to acquire a network address and to inform all other terminals in that sub-net about changes in the network address (terminals that have left, and terminals that have arrived) imposes a heavy load on the system and the terminals. Effectively the overhead required to keep all nodes or terminals up to date about changes in the network can become overwhelming. In a roadway environment, for example, mobile terminals may only be in range of each other for a few seconds, so, not only is it difficult to maintain the network (i.e. keep all nodes up to date about all other nodes), it is often difficult to determine where one network begins and another ends, and if two networks must split or merge, this requires more management overhead still.

In 1995 the US Department of Transportation successfully motivated the Federal Communications Commission to allocate 75 MHz of radio spectrum to be used primarily for vehicular safety applications. To support the use of the spectrum for these applications, and considering the shortcomings of existing communications methods as described above, standards were developed to support the rapid and low latency exchange of messages between vehicles and between vehicles and the infrastructure (see http://www.intellidriveusa.org/library/rept-dsrc-poc.php). This system is known as Dedicated Short Rage Communications (DSRC).

In 2006 the DSRC/WAVE concept was implemented in a proof of concept program funded primarily by the US Department of Transportation. Known as the Vehicle Infrastructure Integration (VII, now IntellDrive[SM]) this system used an interconnected set of fixed roadside DSRC/WAVE units to provide various types of communications to mobile units. Figure 2 shows the architecture of the program's proof of concept system.

The Road Side unit (RSU) is connected via a backhaul link to a service node and through the backbone network to a Service Delivery Node. The individual mobile terminals are connected to other mobile terminals and RSUs in radio range via the DSRC radio link.

DSRC uses seven 10 MHz channels in a 75 MHz band in the 5.9 GHz frequency range allocated by the Federal Communications Commission (FCC). As a result, it offers significant data transfer capacity. However, to make use of this spectrum in a mobile environment required development of new communications protocols. The core radio protocol used is based on the well-known IEEE 802.11a/b/g wireless Ethernet standard, often referred to as Wi-Fi. Because of the unique mobile environment, the 802.11a standard was modified to allow what is known as an "association-less" protocol, identified as IEEE 802.11p. This means that the system does not establish a conventional network with all of the mobile terminals acting as network nodes, maintaining network-level "state" information about each other. The reason this is not done is that the mobile terminals are typically moving, and so they are entering and leaving radio range of each other and various RSUs rapidly. There is typically insufficient time available to set up a new network identity for each new arrival and inform all other nodes in the network before the network changes again because during this process, some terminals may have left, and other new terminals may have arrived. On the surface, this approach may seem to limit the functionality of the system since it means that any given mobile terminal cannot interact uniquely with another terminal (the way computers on an office network might), but this is not the case. Because the system is radio based, all terminals can "hear" all messages transmitted within radio range. So, under most circumstances, one can simply broadcast a message in the local area, and all terminals (mobile terminals and RSUs) can receive it, thus there is no need to establish a low-level network identity. This is particularly useful for safety messaging, since safety information is typically relevant to all terminals in the local area, and with no need for knowing the network identities, a single message can be sent to all terminals within radio range regardless of their network identity (if any). In a typical network addressed environment, one would need to send messages individually to each terminal in range, and this would require knowing which terminals are in range; a complex and inefficient process.

The higher levels of the protocol are defined in a suite of standards known as IEEE 1609 Wireless Access in Vehicular Environments (WAVE). This suite addresses security (1609.2), networking and messaging (1609.3), and channel management (1609.4). In particular, 1609.3 defines a WAVE Short Message Protocol (WSMP) that allows a simple way for a terminal to send messages in the local vicinity. WSMP allows for direct message addressing based on the Medium Access Control (MAC) address of the intended

recipient; however, in practice, most WAVE Short Messages (WSMs) are broadcast and, therefore, are not addressed to any specific recipient.

One skilled in the art will understand that messages may be formed using a variety of data formats, and encoding schemes, such as XML, HTML, SAE J2735, etc and transfer protocols, such as HTTP, HTTPS, SMTP, UDP, TCP/IP, ETC, and security protocols such as HIP, DTLS, VDTLS, IEEE 1609.2, etc.

IP transactions typically require some form of network setup. In the DSRC protocol this setup is implemented by the RSE including its IP address as part of a broadcasted service advertisement or announcement. Once a user terminal has acquired the RSE IP address, it can then create its own IP address (using IPv6 stateless auto-configuration rules) and send IP packets to remote service providers by way of the RSE. The RSE routes these packets through the backhaul network to the Service Delivery Node, through the network gateway to a Virtual Private Network (VPN) via the Internet or a dedicated circuit, and then to the service provider. While somewhat more complex than typical protocols, DSRC achieves the unusual feat of administering communications resources in real time in a way that assures that critical safety messages will have top priority, but that also allows lower-priority messages, both local messages and messages bound for distant servers, to simultaneously use the system. In general, the standard does not describe the use of IP between mobile terminals, but, within the context of an RSE, where proximate terminals have acquired an IPv6 address, this approach is also possible. Other remote IP arrangements are also possible, for example transportable sessions where an ongoing IP session is re-mapped dynamically from one IP address to another as the mobile terminals moves from RSU to RSU.

As useful as the DSRC/WAVE based VII/IntelliDrive^{SM} system is, it still has several significant shortcomings, some of which are shared with the cellular and other IP based systems described above.

In the various addressed network systems describe above (cellular, WiMAX, etc), the terminal must determine its location and then provide the location in geographic coordinates or as geo-referenceable mapping data (e.g. street address, intersection, etc.) to the server that would like to deliver location aware data. This procedure requires a full handshake transaction, whereby the mobile terminal would request certain information from a content server and the content server would deliver the information to that specific terminal. An example for this procedure is the Google maps application on the Apple iPhone, where the phone sends its GPS location to the service provider in order to get the relevant map data for display. Unfortunately, this process is very inefficient since all information for a specific location has to be transmitted n-times for n-terminals.

Collection of data from specific locations is even more complicated and inefficient because the server seeking to collect information from terminals at a specific location must first determine the network addresses of the terminals at that location. This process typically involves transmitting a broadcast message to all terminals in the vicinity of an RSU requesting that they send data about that location.

In addition, there are a few other disadvantages to the solution enabled by current networks:

1. The request-response model requires multiple transactions and therefore takes more time than an information broadcast model.
2. The mobile terminal may change position and an even more complex location resolution process may be necessary in order to find the right communication outlet (cell-tower or RSE) to communicate with the mobile terminal.
3. Since every transaction involves the mobile terminal's IP address, privacy can't be assured by design.
4. If a mobile terminal leaves the coverage area, after making a location base request, but before the response message is received, the message would not be delivered
5. Each message intended for a specific location must be sent uniquely to each terminal in that location, this is exceedingly wasteful of useful radio bandwidth.

A different approach would be to use the existing cell broadcast service in cellular networks. However, there are challenges as well:

1) There are no known solutions to broadcast information in a certain geographic area. Broadcasts over IP networks or cell phone networks reach all users in a local network or cell, but the location of the cell-tower or WiFi outlet is unknown to the service provider when creating the message.
6. Because of the range of the cellular transmitter is so large, the message may reach many mobile terminals that have no need for this information. Each user would have to evaluate the content of a broadcast message to determine if it applies to their current location.

In the VII system described above, to deliver a message to mobile terminals in a particular location, it is necessary to first use an information service to learn the network addresses of the RSUs in that general area. The sender must then decide which of the listed RSUs to send the message to, and then send the message to one or more of the associated addresses. Unless the message is intended only for the immediate vicinity of the addressed RSE, there is no certainty that any of the vehicles passing the addressed RSE will actually pass the location where the message is intended to be delivered. The smaller the number of RSUs the higher the likelihood that the message will not be effectively delivered to vehicles passing the point where it is supposed to be delivered.

Similar issues arise, if a data aggregator wants to collect location aware data from mobile terminals. In this situation each terminal must be programmed to send its data together with embedded location information at regular intervals to a data aggregator. If multiple aggregators want to receive this data, since in these approaches the locations of interest

may change dynamically, it is very difficult to control the sources of the data as they move about. As a result is it typically the case that each aggregator must collect information streams from all users, inspect the messages, and then index and regroup the data entries for processing. Not only is this time consuming, but each data aggregator must then receive all messages, which leads to a massive waste of communication bandwidth.

The alternative is to use a centralized collection and re-distribution function wherein all terminals send data to a single collection point which then serves location and possibly topic specific requests by routing individual components of messages meeting the particular data request (i.e. location or type of data parameter) to secondary users. This approach can be effective, but it suffers from congestion problems at large scales (all messages must pass through one or more choke points, and it raises concerns about privacy, as these centralized hubs are easy targets for wholesale invasions of mobile user's privacy.

It is obvious that today's systems do not provide a convenient method of directly sending data messages to a certain physical location, and do not support the efficient collection certain data messages from specified physical locations.

Summary of the Invention

The present invention addresses the challenges mentioned above.

It is an object of the present invention to avoid these issues by using a new data communications paradigm that uses physical attributes such as location as the basis for message routing.

The present invention describes the relationship and transactions between data/content providers (providers), data/content aggregators (aggregators), network input/output units (network I/O units) that comprise data collection elements and data distribution elements, and mobile terminal units (mobile terminals) to support a novel approach to network data routing based on location and various service attributes.

A network formed according to the present invention resolves internal routing information based on location (coordinates, physical location, logical location, functional or commercial description, etc) attributes of a network I/O unit, or mobile terminal(s) in local proximity of a network I/O unit, such that the sender may send data to the mobile terminal in proximity of the network I/O unit based only on the location attributes of the network I/O unit and the service attributes (type, preferences, authentication, etc) of the mobile unit.

A network formed according to the present invention resolves internal routing information based on location of an network I/O unit, such that the a user may receive data from mobile terminal(s) in proximity of the network I/O unit based only on the location attributes of the Network I/O unit, and the service attributes of the mobile unit.

It is a further object of the current invention that the location and place attributes of a network I/O unit may be provided to the system by the network I/O unit itself, may be provided through a manual entry by a system administrator, or may be automatically acquired through manual or automated cross referencing of the location of the network I/O unit and other geographic an business information.

A network formed according to one embodiment of the current invention provides for a provider to send data to a particular physical location such that network devices in that location can receive such data only as a result of their physical presence at that location and the terminal preferences or authorizations (service attributes). It is a further object of the present invention to allow the provider of such data to describe a location tolerance or range such that mobile terminals within that range may receive such data, but mobile terminals outside that range may not. It is a further object of the present invention that users receiving such data do not need to identify themselves to any elements of the network, and they do not require any form of network identity or address in order to receive such data. It is a further object of the invention that the system may implement various types of authorization and validation to allow a data provider to securely send information to terminals within the area corresponding to the specified location attributes that are also authorized to receive such data.

A network formed according to another embodiment of the current invention provides for a data aggregator to receive data sent from any terminals located at a location specified by the data aggregator that are sending data. It is a further object of the present invention that such a data aggregator may specify a tolerance or range such that it will receive data sent by mobile terminals within that location range or area, and not from mobile terminals not within the specified area. It is a further object of the present invention that users sending such data do not need to identify themselves to any elements of the network, and they do not require any form of network identity or address in order to send such data. It is a further object of the invention that the system may implement various types of authorization and validation to allow a data aggregator to securely receive information from terminals within the area corresponding to the specified location attributes that are also authorized to send such data.

A network formed according to another embodiment of the current invention provides that the sender or receiver of data may specify such location according to a variety of other attributes that may correspond to that location such as place names, coordinates, road intersections, business names, landmarks and other such parameters or attributes. It is a further object of the present invention that such corresponding locations may not be unique, but may correspond to a plurality of locations corresponding to the attributes defined by the sender or receiver, for example specifying the name of a retail outlet might cause data to be sent to the locations of all such retail outlets, or collected from the locations of all such retail outlets.

A network formed according to another embodiment of the current invention provides for the sending of a message to one or more network I/O units nearby the location identified by the location parameters. Mobile terminals receiving the message in the vicinity of any

of the network I/O units, on the basis of their direction of travel and/or proximity to the specified destination location may then re-broadcast this data to other mobile terminals at other locations. In this embodiment, a message communicated in this way will flood the region between the network I/O units and the location identified by the location parameters by being passed from mobile unit to mobile unit until the message is transmitted in the vicinity of the destination location. Such an embodiment would necessarily include mechanisms for managing the re-broadcast of the message to prevent unnecessary re-broadcasting in areas where there are multiple mobile terminals, would include a mechanism for preventing the propagation of the message in directions away from the intended destination, and to limit the overall geographic spread of message re-broadcasting. Such an embodiment would also provide a mechanism for deleting the message after a specified period of time has elapsed, or if the mobile terminal moves sufficiently far away from the specified location. Such an embodiment may also include provision for sending an "anti-message" that, when received by a mobile terminal will terminate the re-broadcast and/or validity of a previously received message subject to such re-broadcasting.

A network formed according to another embodiment of the current invention includes mechanisms for assigning, providing and validating access rights to assure that a sender has authorization to send data of a specified type to or from a specified location, and that a receiver has authorization to receive data of a specified type at or from a specified location.

A network formed according to another embodiment of the current invention supports translation between one form of "addressing" and another. For example: a router that automatically correlates network addresses of Network I/O units with location attributes associated with physical place attributes such as place names, coordinates, landmarks, etc. provided as the destination for the message such that a message bearing a place attribute "address" would be automatically routed to the network address of the outlet or outlets in the vicinity of the place or places that correspond to the place attribute contained in the message.

A network formed according to another embodiment of the current invention allows for a place attribute tolerance or "range" to support delivery of messages to areas or places within a certain range, distance or other attribute similarity to the attribute specified in the message. For example, as described above a particular retail outlet name might be used as an address attribute; according to this embodiment the type of retail outlet may be used instead of the name of the retail outlet, so, for example, a message might be "addressed" to all pizza stores within a geographic region, or all 4-way intersections in a geographic, or jurisdictional region.

A network formed according to another embodiment of the current invention supports place attributes according to a wide range of types such as: Street addresses; street or road intersections; parking structures or lots; shopping centers, zones, or specific retail stores or outlets, including special sales at such locations; sports venues and or events; theme parks or theme park rides, concerts, or other theatrical or entertainment events,

shows and expos such as auto shows, fairs, garden shows, home shows, pet shows etc; and restaurants, including types of cuisine, food courts, etc.

A network formed according to another embodiment of the present invention supports user preferences as service attributes for the transmission or reception of location addressed data. A further object of the present invention is that such service attributes may be acquired from other devices or sources associated with the user, such as personal devices, or personally associated web sites such as MySpace, FaceBook, LinkedIn, etc, or may be set by the user either through a device user interface, or remotely through another interface that can communicate with the device.

Brief Description of the Drawings

Figure 1: Shows a prior art Cellular Data Network
Figure 2: Shows a prior art DSRC Network
Figure 3: Shows a diagram of the present invention System Architecture
Figure 4: Shows a region based diagram of the present invention System Architecture
Figure 5: Shows a region network diagram of the present invention System Architecture
Figure 6: Shows a Message Structure for the present invention.
Figure 7: Shows the Location Header Format structure
Figure 8: Shows Location Encoding Formats
Figure 9: Shows a Service Header Structure
Figure 10: Shows Service Encoding Formats
Figure 11: Shows a typical equipment Architecture of a Location Proxy Server
Figure 12: Shows the flow of events for the location based data distribution function for the preferred embodiment of the present invention.
Figure 13: Shows the flow of events for the location based data collection function for the preferred embodiment of the present invention
Figure 14: Shows the flow of events for the location based message re-broadcast function for the preferred embodiment of the present invention

Detailed Description of Presently Preferred Embodiments of the Invention:

The invention described herein provides a means and function for delivering messages to certain physical locations and for collecting data from certain locations. The approach uses a location header in the communication process that a location aware proxy server can understand to route messages to and from mobile terminals via a variety of wireless and wire-line communication networks.

Referring to Figure 3, the system has the following components.

One or more data content providers (110) and/or data/content aggregators (120) that communicate with one or more mobile networks, preferably using the Internet Protocol (IP) over a broadband backhaul infrastructure (200, 210).

One or more location proxy servers (310, 320, 330) at each mobile network (400, 500, 600), that is aware of the location and/or place attributes of each network information outlet (420,520,620). In an alternate embodiment the proxy server gateway may serve multiple networks and also provide data routing from and to multiple data networks. In yet another embodiment, the proxy server may be integrated with the individual network gateway (410,510,610).

One or more location databases (810) containing address tables that may be used by location proxy server (310, 320, 330) to allow a cross reference between the network addresses of the information outlets and the location and/or place attributes of each network I/O unit. One or more subscriber databases (820) containing information about data/content aggregators (120) relating to service and location attributes of interest. One skilled in the art will understand that the location database(s) may be integrated with the location proxy server, or they may be remotely connected by way of a network, and/or they may be distributed across a plurality of sites. One skilled in the art will also recognize that the function provided by the location database is the location oriented analog of the well known Domain Name Service (DNS).

One or more network gateways for each wireless network (410, 510, 610). The task of the gateway is to route information from the backhaul network(s) to a specific terminal or to a group of terminals within the specific mobile network. The gateway may also be integrated with network I/O unit (e.g. in a WiFi network) and directly connected to the backhaul (e.g. to the Internet), or to an Internet service provider.

A plurality of network I/O units including, but not limited to DSRC roadside units (RSU 420), cellular towers (520), and WiFi hot spots (620), each fixed at a certain location, and each associated with at least a location oriented place attribute, and in some embodiments additional place attributes. These Network I/O units directly communicate with the mobile terminals over a wireless transceiver and are connected to the gateway via open or proprietary backhaul networks (430, 530, 630). One of skill in the art would recognize that the wireless networks could be of any type that supports addressed or broadcast data communications, and that systems that support one or another type of broadcast or multicast would be the most effective.

A proprietary and/or open standard backhaul network (210, 430, 530, 630), connecting the information outlets to the proxy server, by way of the network gateways.

A number of mobile terminals (700), which may connect to one or more wireless networks using either addressed or broadcast communications.

It will be appreciated that The location aware proxy server abstracts the knowledge of the specific wireless infrastructure; messages are sent to locations not to addresses, so no knowledge of the proprietary wireless communication network or the locations of the network I/O units (e.g. Wifi hot spot, cell tower, or other roadside equipment) is necessary. This means that using this system:

a. Physical configuration of network can change without changing addressing to information outlets and mobile terminals. The message originator has not to know about any changes in the network
b. Service providers and data collectors only need to know how to reach proxy servers. Data collectors acquire information from a physical location without knowing network infrastructure
c. Messages can be directed to location over multiple networks simultaneously

The architecture may further be organized in different hierarchies. Figure 4 shows a main proxy server 300 that distributes information to different regions, each represented by a regional proxy server (301, 302, or 303). Each regional proxy server distributes information to the appropriate network gateways (410, 510, and 610). In the same way, the regional proxy servers forward collected information via the main proxy server to subscribers of collected information.

Figure 5 shows an alternate embodiment of the same concept, where the information is first split up by network technology and then by region.

The generic operation of the system for distribution of location oriented messages is described as follows, referring to Figures 3, 6, and 12.

Location Based Data Distribution:

1) At step 1500 of Figure 12, the Data Content Provider (110) creates a data payload message (1400) to be distributed to mobile terminals at a certain location.
2) At step 1510, in order to provide the message to only valid terminals, a service header (1300) may be added to describe the type of service and any attributes relevant for service delivery.
3) At step 1520, Data Content Provider (110) adds a location header (1200) and Location Proxy address header (1100) to this message. The location header (1200) includes the location type (e.g. point, area, road link), encoded location data (e.g. latitude / longitude, x-y, or other geographical coordinates) and/or additional parameters (e.g. road link ID, feature ID, attribute ID) to address the payload message (1300) to a certain location.
4) At Step 1530, Data Content Provider (110) sends the message to the appropriate Location Proxy Server (310, 320, 330) which may be addressed by using a TCP/IP or UDP/IP address header or any other networking address header (1100).
5) At step 1540, Location Proxy Server (310, 320, 330) receives the message (1000) via network (210) from content server (120) and extracts the location header along with the service header and payload message.

6) At step 1550, Location Proxy Server (310, 320, 330) examines headers (1200, 1300), and using information in Location Database (810), determines the network addresses of the relevant Network I/O units (420, 520, 620) based on the location encoded information in the Location header (1200) and service attributes in Service Header (1300);
7) At step 1560, Location Proxy Server (310, 320, 330) forwards the message to the appropriate network I/O units (420, 520, 620) via the network gateway (410, 510, 610) and one of the communication links (430, 530, 630) using network addressing information determined in step 1550.
8) At step 1570a, Network I/O Unit (420, 520, 620) broadcasts the information to all local mobile terminals in communication range.
   Alternately, at step 1570b, one or more of the Network I/O Units (420, 520, 620) may also send the message individually to the current network addresses of mobile terminals known to be in communications range of the Network I/O Unit.
9) At step 1580, Mobile Terminal (700) receives the message broadcast from, or sent by, Network I/O Unit (420, 520, 620).
10) At step 1590, Mobile Terminal (700) performs actions based on Message Payload (1400), or Header Data (1200, 1300). As shown in steps 1591a through 1591d, such actions may include, singly, collectively, and in any order:
    Step 1591a: Display of certain elements of the message content in the form of text, images or video;
    Step 1591b: Generation of audio information related to or derived from he message content;
    Step 1591c: Production of other types of user interface signals usable by the mobile terminal or its peripheral devices or interfaces;
    Step 1591d: Generation and transmission of another message bearing content headers (1100, 1200, 1300), related to, but not necessarily the same as the received message;
    Step 1591e: Control of one or more terminal application functions based on the information in the content headers (1100, 1200, 1300); For example, requesting additional terminal specific information from the Network I/O Unit (420, 520, 620), such as security information; decrypting received content, Holding the message until some other criteria is met (for example the location of the mobile unit is within a geographic region specified in the message, or a specific time elapses, etc), and then talking one or more of the actions described in steps 1591a through 1591d, etc. Such actions may also include comparison of the message header information and or message content information to stored user preferences to determine the appropriate actions, which may include no action.

The generic operation of the system for collection of location oriented messages is described as follows, referring to Figures 3, 6, and 13.

Location Based Data Collection:

1) At step 1600, the Mobile Terminal (700) sends a data message to local Network I/O Units (420, 520, 620). In an alternative embodiment, the mobile terminal may also broadcast the information to other mobile terminals in the same local network or available through ad-hoc networking. In yet another embodiment, the mobile terminal may use a positioning system such as GPS and or a digital map to determine its location and add the location type (e.g. point, area, road link), location data, (e.g. latitude / longitude, x-y, or other geographical coordinates) and as well as additional parameters (e.g. road link ID) to the message header of such a data message. As shown in steps 1601a through 1601e Mobile Terminal (700) my generate such data messages on the basis of a variety of events, such as:
   Step 1601a: A request by the Network I/O Unit (420, 520, 620);
   Step 1601b: Location within a specified geographic region;
   Step 1601c: Location within a particular place identified by a name, encoded name number or symbol or other place attribute;
   Step 1601d: Time of day, or time elapsed since the last data transmission;
   Step 1601e: Accumulated data associated with a parameter associated with the Mobile Terminal (700) reaching a pre-determined threshold (quantity, value, event, etc). One skilled in the art will recognize that the parameters associated with mobile device (700) may include operating parameters for the device or the user, or a vehicle in which the Mobile Terminal (700) is either embedded, connected or being carried;
   Step 1601f: Reception of a data trigger message from another mobile device (700) or from a device located in proximity to, or integrated with Network I/O Unit (420, 520, 620);
2) At step 1610, Network I/O Unit (420, 520, 620) receives message (1000) and adds its location information to all messages received from local mobile terminals (700);
3) At step 1620; Network I/O Unit (420, 520, 620) sends the message via the Network Gateway (410,510,610) to the Location Proxy Server (310, 320, 330); It should be understood by one skilled in the art that Network I/O Unit (420, 520, 620) may also aggregate a plurality of messages received either from a single Mobile Device (700) or from multiple Mobile Devices (700), and send the aggregated data as an aggregate message to the Location Proxy Server (310, 320, 330);

4) At step 1630, Location Proxy Server (310, 320, 330) receives the message(s) sent by the Network I/O Unit (420, 520, 620);
5) At step 1640, Location Proxy Server (310, 320, 330) examines the message headers (1100, 1200, 1300), and using data/content aggregator subscriber Database (820), determines the addresses of relevant data aggregators based on their subscription to location encoded information;
6) At step 1650, Location Proxy Server (310, 320, 330) distributes the received messages to the appropriate Location Data Aggregators (120) (via backhaul connection (210). One of skill in the art will recognize that, depending on the contents of Location Subscriber Database (820), Location Proxy Server (310, 320, 330) may distribute all messages with the specified location and content information to a data/content aggregator or it may distribute portions of those messages;
7) At step 1660, Data/Content Aggregator(s) (120) receive data messages for further processing.

Assuming a Mobile Terminal (700) has received and acted on a message generated by a Data/Content Provider (110) as described in connection with Figure 12 (e.g. received and displayed the message), the present invention provides a mechanism for Mobile Terminals (700) to distribute such received messages independently of the presence of Network I/O Units (420, 520, 620). This is described as a further action taken by Mobile Terminal (700) as follows, referring to Figures 3, 6, and 14:

Location Based Data Re-Broadcast:

Assuming a Mobile Terminal (700) has received Message (1000) generated by a Data/Content Provider (110) as described in connection with Figure 12:

1) At step 1700, Mobile Terminal (700) waits to receive a message;
2) At step 1710a, Mobile Terminal (700) receives Message (1000) broadcast from, or sent by, Network I/O Unit (420, 520, 620) (Note: This is the same as Step 1580 of Figure 12).
   Alternatively, at step 1701b, Mobile Terminal (700) receives a Message (1000) broadcast from, or sent by another Mobile Terminal within wireless radio range of Mobile Terminal (700).
3) At step 1720, Mobile Terminal (700) examines Header (1100, 1200, 1300), and/or Message Payload (1400), and determines that the message is designated for re-broadcast;
4) At step 1730, Mobile Terminal (700) compares Header (1100, 1200, 1300), and/or Message Payload (1400), to a list of cancelled re-broadcast messages received at some earlier time; If the Message (1000) has been cancelled, Mobile Terminal (700) deletes the received message, and returns to step 1700; If not, then it proceeds to step 1740;

5) At step 1740, Mobile Terminal (700) generates a random number between -200 and +200, and adds this to re-broadcast repeat interval information contained in the Service Header (1300) measured in milliseconds, this new value is referred to as the Local Repeat Interval; One skilled in the art will recognize that the value of the random number added to the re-broadcast repeat interval depends on the type of network, and that other values could be used to optimize performance based on the transmission and message processing time of the wireless network and the Mobile Terminals;
6) At step 1750, Mobile Terminal (700) compares message headers (1100, 1200, 1300), and/or message payload (1400) to any messages received since the subject message was received, if no received messages are the same as the subject message, then the mobile Terminal (700) proceeds to step 1760. If the subject message has been subsequently received after its initial reception, the Mobile Terminal (700) returns to Step 1730.
7) At step 1760, the Mobile Terminal compares the Local Repeat Interval to the time elapsed since it last received the same Message (1000) or transmitted the same Message (1000); If the time elapsed since receiving or transmitting the Message (1000) is equal to or greater than the re-broadcast repeat interval, the Mobile Terminal (700) proceeds to step 1760; If not, it returns to step 1730 (i.e. it waits for the Local Repeat Interval to expire);
8) At step 1770, Mobile Terminal (700) compares the re-broadcast time expiry information contained in the Service Header (1300) to the current time; If the re-broadcast expiry time is after the current time, it proceeds to step 1780, otherwise it deletes the message and returns to step 1700;
9) At step 1780, Mobile Terminal (700) compares the re-broadcast region information contained in the Location Header (1200) to its current location; if Mobile Terminal (700) is inside the re-broadcast region, it proceeds to step 1790; if not, it returns to step 1730; One skilled in the art will understand that in the preferred embodiment, the re-broadcast region will preferably be geographically separate from the reception region in the vicinity of the Network I/O Unit (420, 520, 620);
10) At step 1790, Mobile Terminal (700) broadcasts Message (1000), and returns to step 1730.

Following steps 1700 to 1780 of the process described above and illustrated in Figure 14, the present invention will cause messages to be re-transmitted by mobile Terminals (700) to other mobile terminals (700) within radio range at regularly specified intervals within the re-broadcast region. If Message (1000) has been re-broadcast by another Mobile Terminal (700), then all Mobile Terminals (700) receiving such broadcast will reset their re-broadcast timers and continue to wait; If they receive a cancellation message, or if the message expires, then they will exit the process; If the Mobile Terminal (700) is not

within the re-broadcast region, then it will hold the message until it is cancelled, or it expires, or until the Mobile Terminal re-enters a the re-broadcast region. If the message is not expired or cancelled, and the Mobile Terminal is inside the re-broadcast region, then when the local repeat interval expires it will re-transmit the message. In this way, the message will continue to be broadcast and spread geographically throughout the re-broadcast region as long as Mobile Terminals (700) are present. One skilled in the art will also appreciate that if the broadcast region surrounding network I/O units (420, 520, 620) is not the same as the re-broadcast region, this process will cause the effective broadcast region for the message to be the geographic union of both regions, or will cause the message to be broadcast in two distinct regions, one in the vicinity of the network I/O units (420, 520, 620), and one at another defined location where there is not necessarily an network I/O unit (420, 520, 620).

In addition, the system allows for integration of the Location Proxy Server (310, 320, 330) function with the network gateway (410, 510, 610). Alternatively, one Location Proxy Server routes location aware messages to multiple independent Networks (400, 500, 600).

It will be appreciated by one of skill in the art the range of the network I/O units (420, 520, 620) may be such that a mobile terminal (700) in any given location may be able to communicate with multiple network I/O units (420, 520, 620), and that such a situation will require additional processing to detect duplicate messages receive from two or more network I/O units (420, 520, 620). Similarly, the broadcast of data from a mobile terminal (700) in any given location may be received by multiple network I/O units (420, 520, 620), and that the location proxy server (310, 320, 330) or the data aggregator (120) may require additional processing to eliminate duplicate messages. Alternatively, the mobile terminal (700) may identify the closest network I/O unit (420, 520, 620) using, for example the location of the network I/O unit (420, 520, 620) as included in or appended to the message by the network I/O unit (420, 520, 620) and compared to the location of the mobile terminal (700) as determined using global positioning system (GPS), time difference of arrival (TDOA), angle of arrival (AOA), received signal strength measurements or other positioning schemes. Such positioning schemes may be independent of the network I/O units (420, 520, 620) (i.e. self contained in the mobile terminal) or they may be cooperative, wherein the stationary network I/O units (420, 520, 620) each measure signal strength of each other and/or the mobile terminals, and provide information to the mobile terminals to aid in determining the relative position of the mobile terminal to the network I/O units.

The current invention may support a wide variety of mobile communication networks, including WiFi hotspots (IEEE 802.11), Wimax (IEEE 802.16), ad hoc networks (based on 802.11 or 802.11 derivatives such as DSRC, cellular networks (2G: CDMA, GSM; 2.5G: GPRS, 1xRT, EDGE; 3G: CDMA-2000, WCDMA, UMTS; 4G: LTE).

The location data in the location header maybe encoded in many different types and formats. Figure 7 shows one preferred mode of encoding location by referring to a

location ID (1210) for better cross referencing, a location type (1220) to specify the location data format, the location data (1230), and the time (1240).

Figure 8 shows a list of different location types and their respective data formats. This list is intended to give someone skilled in the art a good understanding how to implement various location type and data combinations. A point may be encoded by referring to a landmark, a street address, an intersection of two roads, by a mile-post and offset or geographical coordinates. An area may be encoded by ZIP code, political borders such as county, state, or country, and by referring to road segments. There are many data formats that can be used to encode a specific location a road, or an area. For this purpose the Geographic Data Format (GDF 3.0), a CEN and ISO standard for encoding location data is incorporated hereby included by reference.

Other standards include the ISO 3166 specification, the OpenGIS KML 2.2 *Encoding Standard* (OGC KML), CityGML, POI XML, RDF™, SIF+, and IETF RFC1712 (http://www.faqs.org/rfcs/rfc1712.html). In addition, there are private vendor encoding standards such as Navteq NN4D and NAVSTREETS® data format.

Locations may also be encoded abstractly using business type references such as North American Industry Classification System (NAICS) codes, stock exchange symbols, or other identifying references. Such references may also be combined with other location references such as city, state or county to reference businesses of a particular type or brand within a given geographic or jurisdictional region.

Figure 9 shows an embodiment of a service header. The service header consists of a service identifier and one or more service attributes associated with that service identifier. In this example, the urgency of the message is one attribute, which is encoded with a value of "HIGH".

As shown in Figure 10, other service attributes may include any information that is relevant for handling of the message payload by the mobile terminal. For example, the service header information may include preference information established by the user of the mobile terminal so that messages may be filtered according to the user's needs or interests. This information may include various authorizations so that, for example only users with approved credentials may receive certain broadcast messages. These authorizations may be implemented in multiple ways. For example a general broadcast to a local area regarding a person in that area in need of medical attention may be encrypted such that only mobile terminal users with appropriate training can decrypt the message and thereby be notified of the need should they choose to provide assistance. Such an authorization system might use a digital key provided to the user based on their certification, or their mobile terminal may be instructed to contact a clearing center to provide specific information prior to be sent a decryption key. In less critical situations, the service header information may include, for example membership information so that messages relevant to specific membership levels can be targeted only at members of that level. Such a system might be useful, for example to issue information or instruction messages at an airport directing elite mileage club members to one place, while directing

other level members to another. The same mechanism may be used, for example in a shopping mall, where messages are filtered on reception by comparing the service header information to the user profile data in the mobile terminal. In this application, messages targeted at teens would be received by mobile terminals belonging to teens, while elderly shoppers might receive messages targeted to their specific needs or interests.

One of skill in the art will appreciate that the location header and service header may be implemented such that they can be extended to provide a wide variety of different ways to encode or reference different types of location or service related information.

Figure 11 shows the hardware of a typical proxy server apparatus. The proxy server typically uses a microprocessor (4100) to execute Software (4200). The microprocessor has access to non-volatile and volatile memory for storing the software (4200) and providing storage for program data and communication caching. The proxy server may be further connected to one or more communication networks using one or more network interfaces (4600). The proxy server may further have a real-time clock to process messages based on attributes such as time stamps and urgency.

The main function of the software (4200) is to provide efficient routing of messages from data providers to mobile terminals or from mobile terminals to data aggregators.

Although the disclosed embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made to the embodiments without departing from their spirit and scope.

The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or element of the present invention. Accordingly, the present invention is not intended to be limited to the specific form set forth herein, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents, as can be reasonably included within the spirit and scope of the invention as provided by the claims below.

Claims:

We claim anything and everything described herein.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	System and Method for Information Distribution and Collection in Location Based Communication Networks
First Named Inventor/Applicant Name:	Scott Sturges Andrews
Filer:	Scott Andrews
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**82**

Electronic Acknowledgement Receipt

EFS ID:	9565101
Application Number:	13038335
International Application Number:	
Confirmation Number:	8621
Title of Invention:	System and Method for Information Distribution and Collection in Location Based Communication Networks
First Named Inventor/Applicant Name:	Scott Sturges Andrews
Correspondence Address:	Scott Andrews - 915 Western Ave. - Petaluma CA 94952 US 650-279-0242 scott@cogenia.com
Filer:	Scott Andrews
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	01-MAR-2011
Filing Date:	
Time Stamp:	20:56:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$82

RAM confirmation Number	7503
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Specification	System_and_Method_for_Information_Distribution_and_Collection_in_Location_Based_Comm_Networks.pdf	1162644 0dc75c6e0bc039b197f450adf1615b8162239fcb	no	30
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	29375 0b1459ce24d9c5ef4929a5c17dfdb9d0f54c8763	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1192019		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

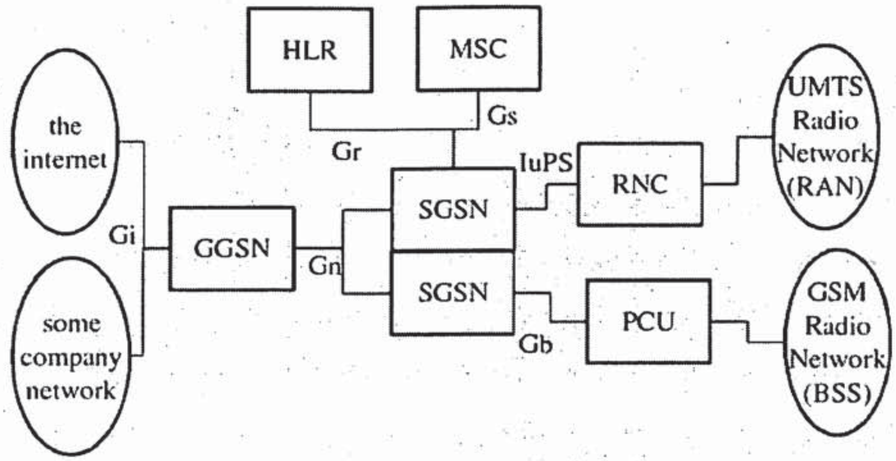

Figure 1: Prior Art Cellular Data Network

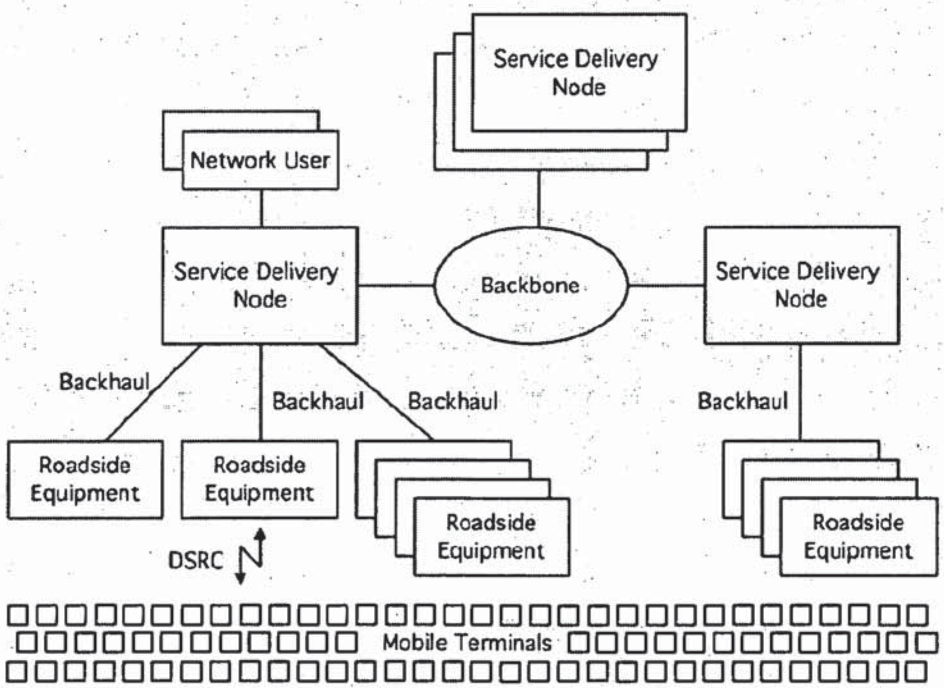

Figure 2: Prior Art DSRC Network

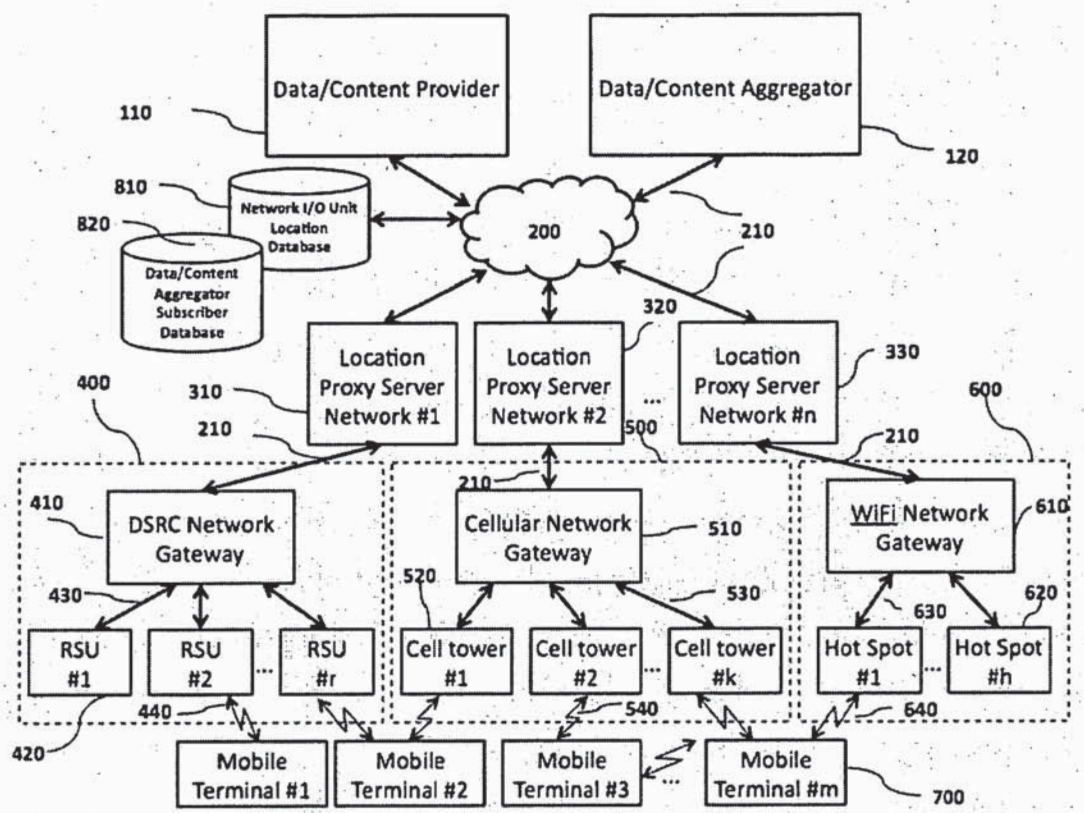

Figure 3 System Architecture

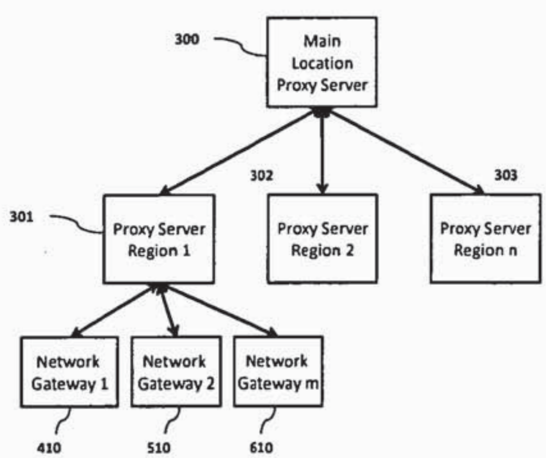

Figure 4: Hierarchical information distribution and collection by region.

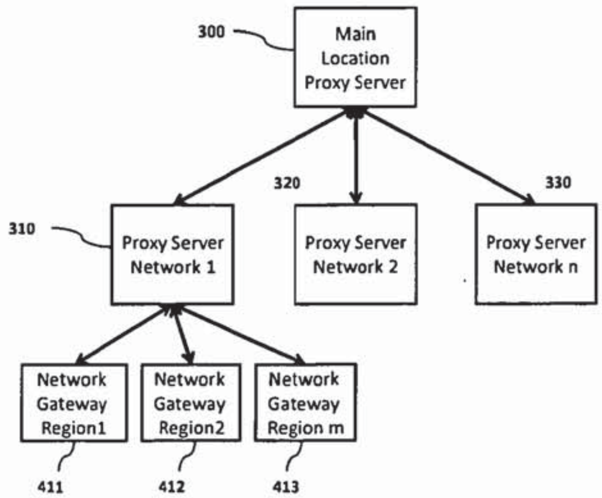

Figure 5: Hierarchical information distribution and collection by network technology.

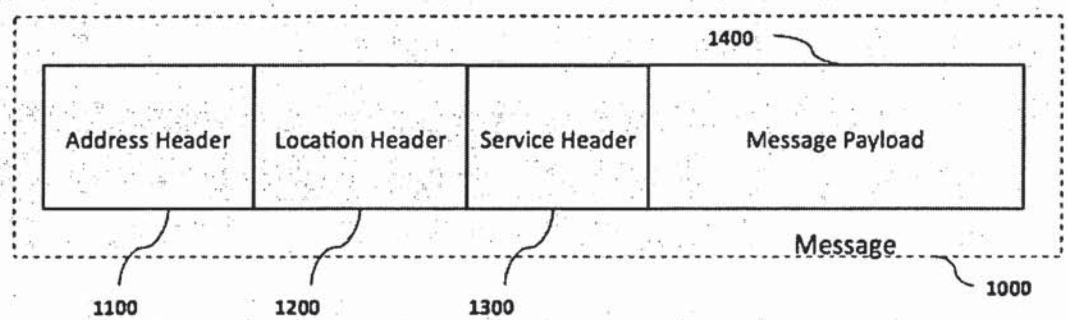

Figure 6: Message Structure

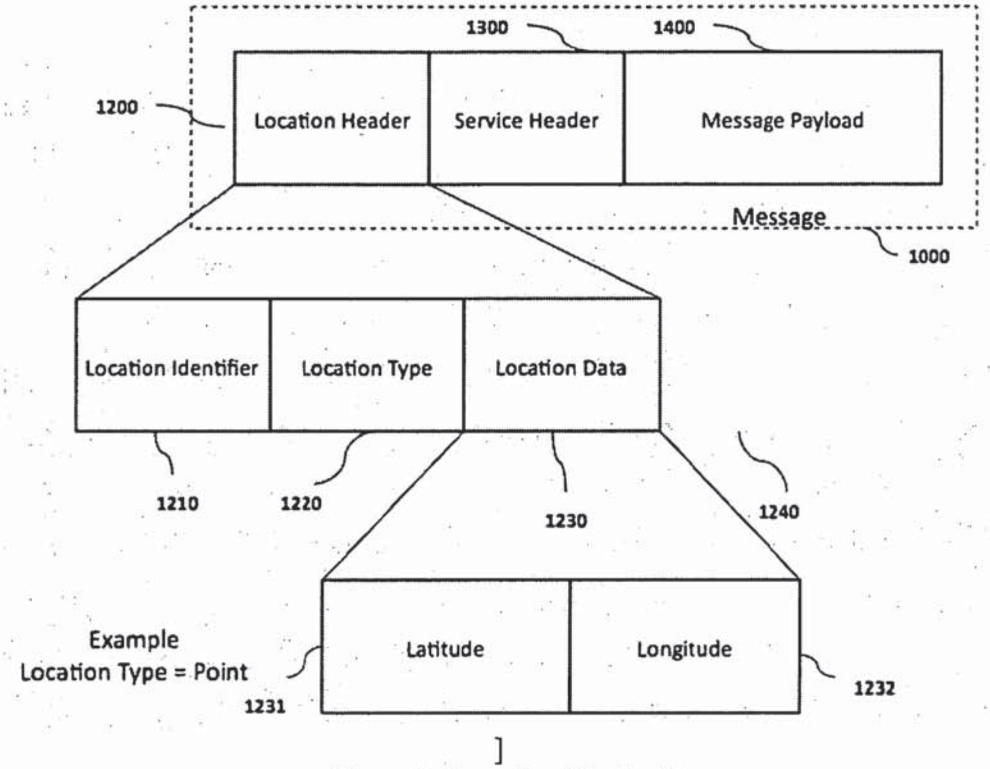

Figure 7: Location Header Formats

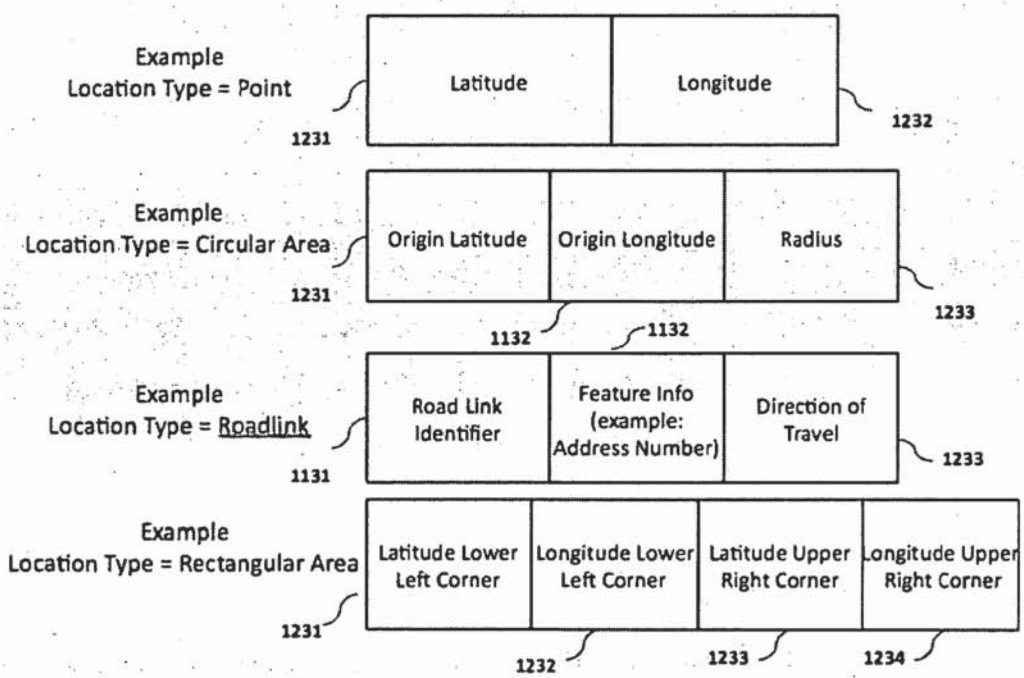

Figure 8: Location Encoding Formats

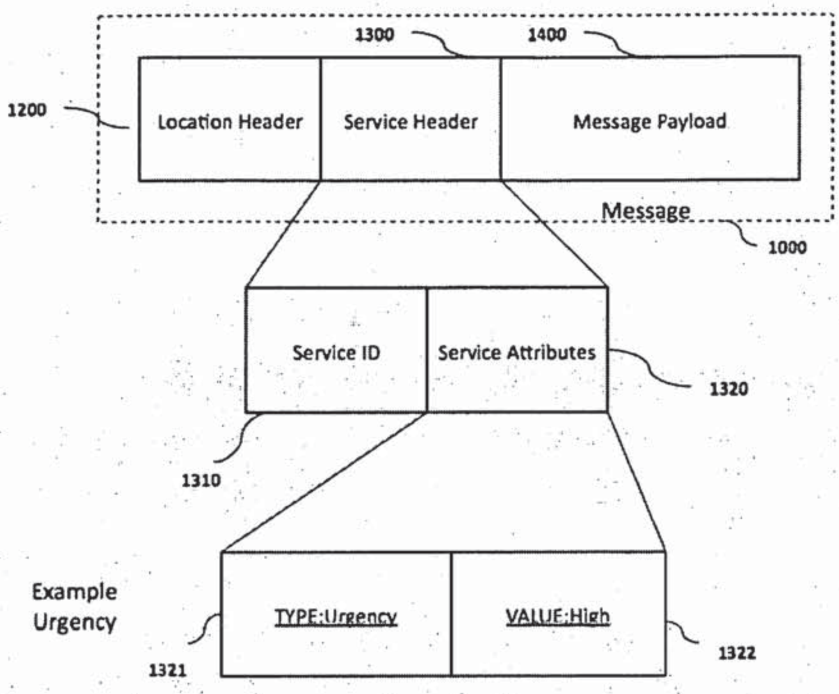

Figure 9 Service Header

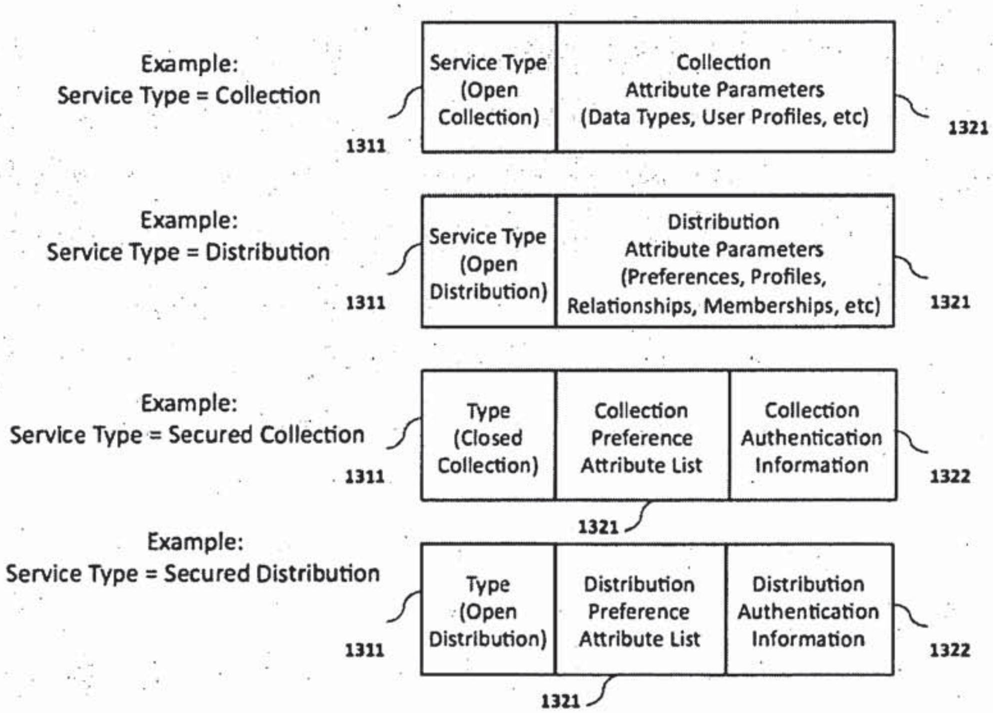

Figure 10 Service Encoding Formats

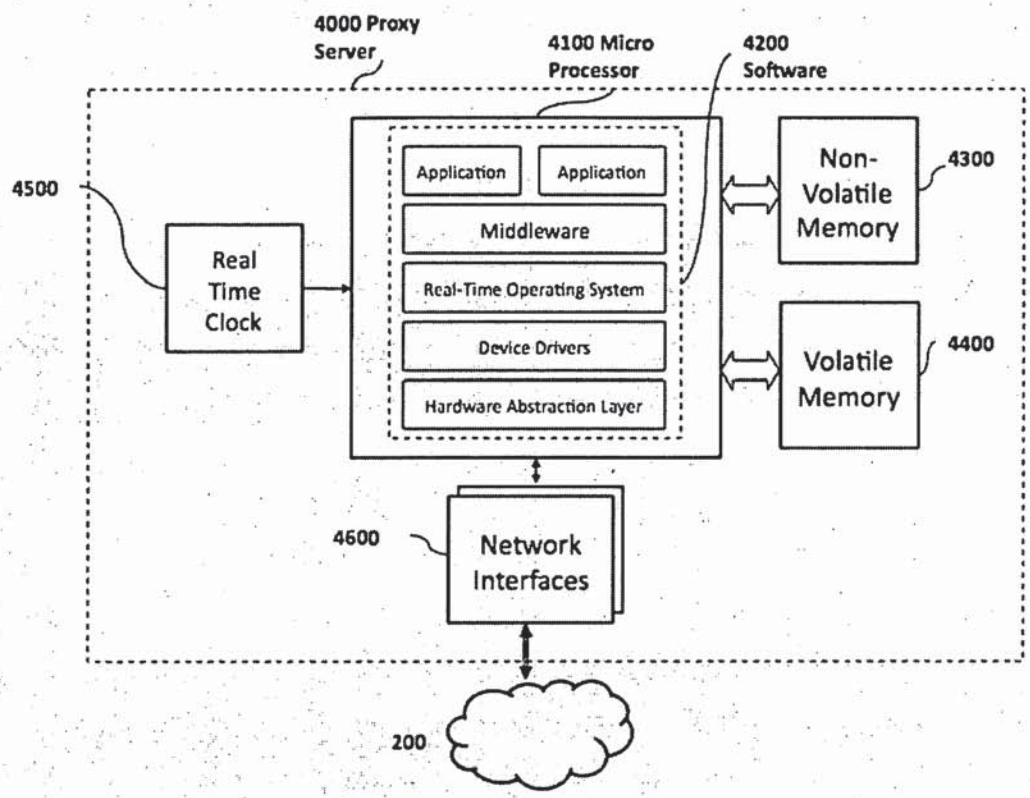

Figure 11 Hardware of a Typical Location Proxy Server Apparatus

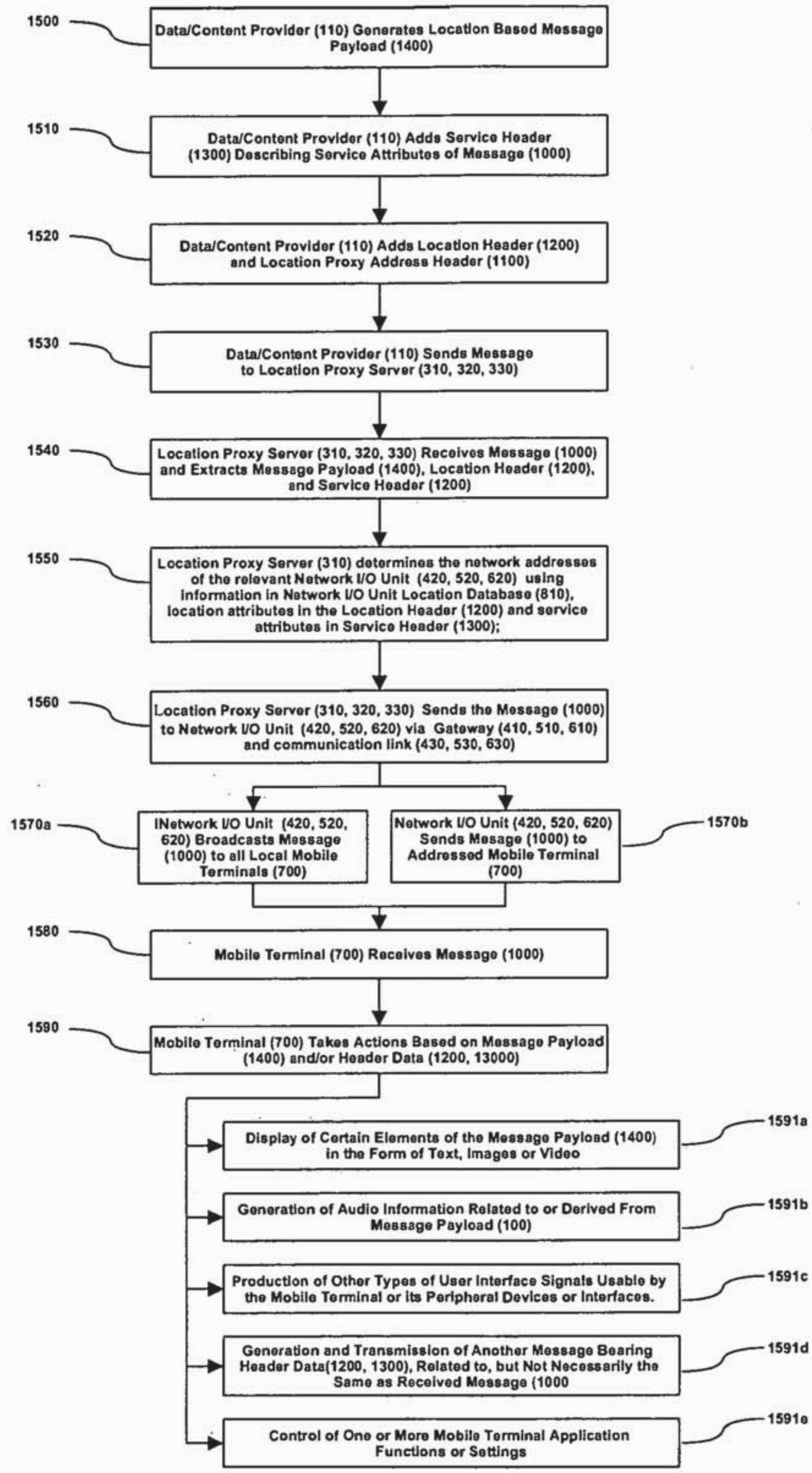

Figure 12 Data Distribution Process

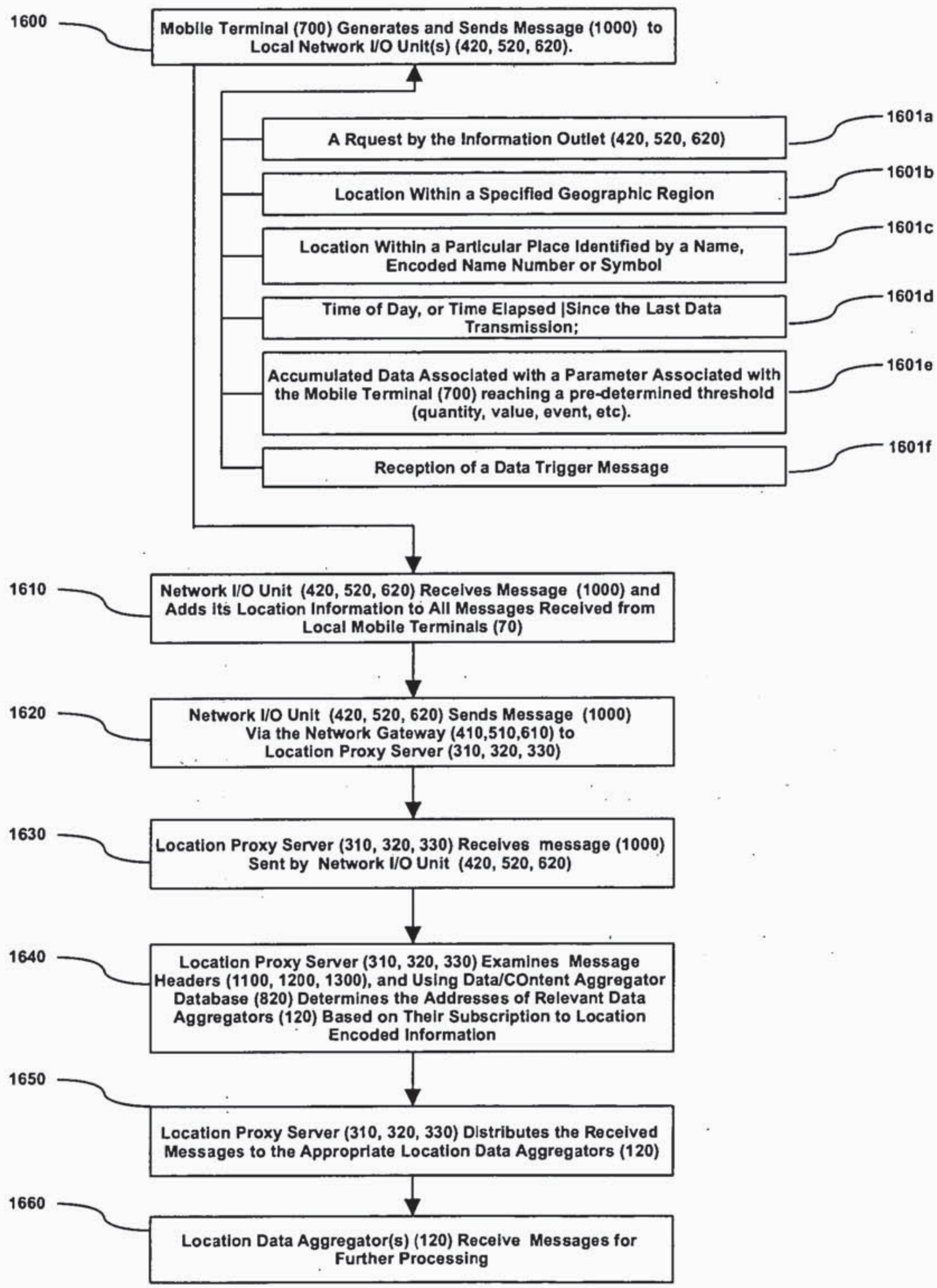

Figure 13 Data Collection Process

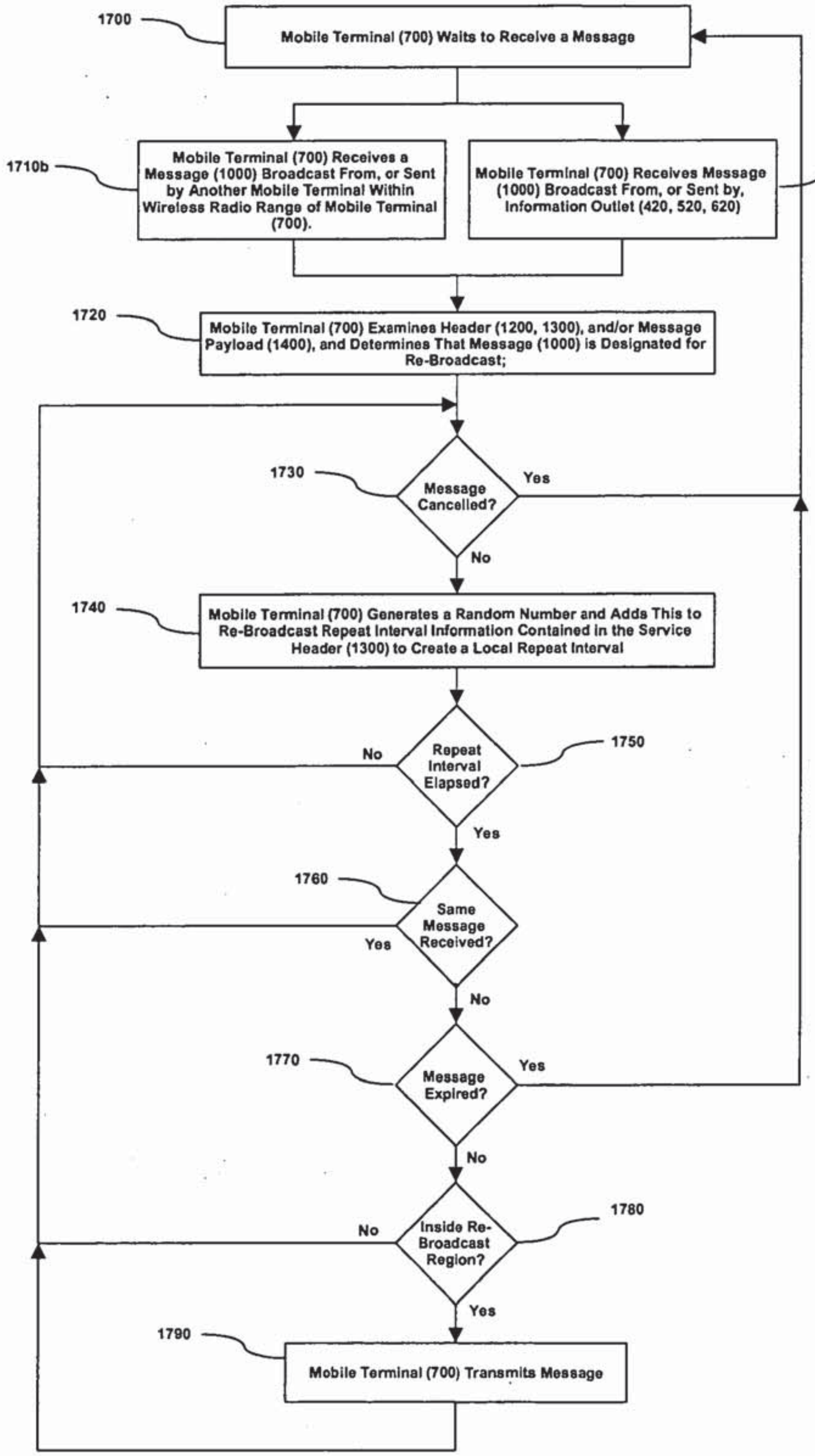

Figure 14 Data Re-Broadcast Process